IN THE CLAIMS

Please cancel claims 1-39 without disclaimer or prejudice to be pursued in this or a later-filed continuation or continuation-in-part application and add the following new claims.

1 - 39. (Canceled)

40. (New) A system for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

a switching system that provides a network address of the second network device to the first network device, said switching system receiving the information packets from the first network device and directing the information packets to the second network device;

a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and

a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets are problematic, identifying the abnormal information packets as being the problematic information packets and inhibiting said switching system from providing the network address of the second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

41. (New) The system of claim 40, wherein said switching system includes a routing system.

42. (New) The system of claim 40, wherein said route arbitration system is at least partially incorporated into said switching system.

43. (New) The system of claim 40, wherein said route arbitration system communicates with said switching system via at least one communication link selected from the group consisting of a remote monitoring network probe, a switching device, and an Ethernet probe.

44. (New) The system of claim 40, wherein said route arbitration system monitors a volume of the information packets.

45. (New) The system of claim 44, wherein said route arbitration system determines that the information packets comprise said abnormal network activity when the volume of the information packets is greater than a preselected volume threshold level.

46. (New) The system of claim 40, wherein said route arbitration system, upon determining that the information packets no longer comprise said abnormal network activity, enables said switching system to again provide the network address of the second network device to the first network device and receive the information packets from the first network device.

47. (New) The system of claim 40, wherein said traffic analysis system is at least partially incorporated into said switching system.

48. (New) The system of claim 40, wherein said traffic analysis system monitors a volume of the abnormal information packets.

49. (New) The system of claim 48, wherein said traffic analysis system determines that the abnormal information packets are problematic when the volume of the abnormal information packets is greater than a preselected volume threshold level.

50. (New) The system of claim 48, wherein said traffic analysis system determines that the abnormal information packets are problematic when the volume of the abnormal information packets does not decrease during a preselected time interval.

51. (New) The system of claim 40, wherein said traffic analysis system instructs said switching system to redirect the information packets to a null network device having a null address, said null network device receiving the information packets and providing no response to the first network device.

52. (New) The system of claim 52, wherein said traffic analysis system instructs said switching system to provide said null address to the first network device such that the first network device transmits the problematic information packets to said null network device.

53. (New) The system of claim 52, wherein said null network device is provided by at least one of said route arbitration system and said traffic analysis system.

54. (New) The system of claim 40, further comprising a firewall system that identifies suspect information packets received from the first network device, said switching system directing the information packets to the second network device via said firewall system.

55. (New) The system of claim 54, wherein said traffic analysis system determines whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic, inhibits said switching system from providing the network address of the second network device to the first network device.

56. (New) A system for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

a switching system that provides a network address to the first network device, said switching system receiving the information packets from the first network device and directing the information packets to the second network device; and

an activity monitoring system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets are problematic in accordance with at least one predetermined criteria and, if said activity monitoring system determines that the information packets are problematic, identifying the information packets as being the problematic information packets and inhibiting said switching system from providing the network address of the second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

57. (New) The system of claim 56, wherein said activity monitoring system monitors a volume of the information packets and determines that the information packets are problematic when the volume of the information packets is greater than a preselected volume threshold level.

58. (New) The system of claim 57, wherein said activity monitoring system monitors a volume of the information packets that exceed said preselected volume threshold level and determines that the information packets are problematic when the volume of the information packets exceeding said preselected volume threshold level does not decrease during a preselected time interval.

59. (New) The system of claim 56, wherein said activity monitoring system includes:

a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and

a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets comprise the problematic information packets in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets comprise the problematic information packets, inhibiting said switching system from providing the network address of the second network device to the first network device.

60. (New) A system for identifying and diverting problematic information packets received from an external network device, comprising:

a protected network device having a network address;

a switching system that provides said network address to the external network device, said switching system receiving the information packets from the external network device and directing the information packets to said protected network device;

a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and

a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets are problematic, identifying the abnormal information packets as being the problematic information packets and inhibiting said switching system from providing the network address of said protected network device to the external network device,

wherein said switching system, when inhibited, renders said protected network device unreachable and prevents the external network device from transmitting the problematic information packets to said switching system.

61. (New) The system of claim 60, wherein said protected network device comprises at least one network device selected from the group consisting of a server system, a computer system, a provider computer system, a user computer system, a router system, an edge router system, a core router system, and a firewall.

62. (New) The system of claim 60, further comprising a communication system, said switching system communicating with the external network device via said communication system.

63. (New) The system of claim 62, wherein said communication system comprises a communication link selected from the group consisting of a local area network, a wired communication network, a wireless communication network, a wide area network, a public communication network, and the Internet.

64. (New) The system of claim 60, wherein said route arbitration system monitors a volume of the information packets and determines that the information packets comprise said abnormal network activity when the volume of the information packets is greater than a preselected volume threshold level.

65. (New) The system of claim 60, wherein said route arbitration system, upon determining that the information packets no longer comprise said abnormal network activity, enables said switching system to again provide the network address of the protected network device to the external network device and receive the information packets from the external network device.

66. (New) The system of claim 60, wherein said traffic analysis system monitors a volume of the abnormal information packets and determines that the abnormal information packets are problematic when the volume of the abnormal information packets is greater than a preselected volume threshold level.

67. (New) The system of claim 60, wherein said traffic analysis system monitors a volume of the abnormal information packets and determines that the abnormal information packets are problematic when the volume of the abnormal information packets does not decrease during a preselected time interval.

68. (New) The system of claim 60, wherein said traffic analysis system instructs said switching system to redirect the information packets to a null network device having a null address, said null network device receiving the information packets and providing no response to the external network device.

69. (New) The system of claim 60, further comprising a firewall system that identifies suspect information packets received from the external network device, said switching system directing the information packets to the protected network device via said firewall system, said traffic analysis system determining whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic, inhibiting said switching system from providing the network address of the protected network device to the external network device.

70. (New) The system of claim 60, wherein said traffic analysis system instructs said switching system to redirect the information packets to a traffic analysis device, said traffic analysis device receiving and analyzing the information packets.

71. (New) A method for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

providing a network address of the second network device to the first network device via a switching system receiving the information packets from the first network device and directing the information packets to said second network device;

monitoring the information packets received from the first network device;

determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria;

if the information packets are determined to comprise abnormal network activity, identifying the information packets as being abnormal information packets;

monitoring the abnormal information packets;

determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria; and

if the abnormal information packets are determined to be problematic,

identifying the abnormal information packets as being the problematic information packets; and

inhibiting said switching system from providing the network address of said second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

72. (New) The method of claim 71, wherein said monitoring the information packets includes monitoring a volume of the information packets and wherein said determining whether the information packets comprise said abnormal network activity includes determining that the information packets comprise said abnormal network activity when the volume of the information packets is greater than a preselected volume threshold level.

73. (New) The method of claim 71, wherein said monitoring the abnormal information packets includes monitoring a volume of the abnormal information packets and wherein said determining whether the abnormal information packets are problematic includes determining that the abnormal information packets are problematic when the volume of the abnormal information packets does not decrease during a preselected time interval.

74. (New) The method of claim 71, further comprising determining that the information packets no longer comprise said abnormal network activity and enabling said switching system to again provide the network address of the second network device to the first network device and receive the information packets from the first network device.

75. (New) The method of claim 71, wherein said inhibiting said switching system includes redirecting the information packets to a null network device having a null address, said null network device receiving the information packets and providing no response to the first network device.

76. (New) The method of claim 75, wherein said redirecting the information packets includes instructing said switching system to provide said null address to the first network device such that the first network device transmits the problematic information packets to said null network device.

77. (New) A method for identifying and diverting problematic information packets transmitted from a first network device to a second network device, comprising:

providing a network address of the second network device to the first network device via a switching system receiving the information packets from the first network device and directing the information packets to said second network device;

monitoring the information packets received from the first network device;

determining whether the information packets are problematic in accordance with at least one predetermined criteria; and

if the information packets are determined to be problematic,

identifying the information packets as being the problematic information packets; and

inhibiting said switching system from providing the network address of said second network device to the first network device,

wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system.

78. (New) The method of claim 77, wherein said determining whether the information packets are problematic includes:

determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria;

if the information packets are determined to comprise abnormal network activity, identifying the information packets as being abnormal information packets;

monitoring the abnormal information packets; and

determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria.